

**Notice of Allowability**

Application No.

10/661,341

Examiner

Laurel Lashley

Applicant(s)

MEYER ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 07/30/07.
2. ☒ The allowed claim(s) is/are 1-6 and 10-21.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All   b) ☐ Some\*   c) ☐ None   of the:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |   |
|--|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application                     |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 7. <input type="checkbox"/> Examiner's Amendment/Comment                              |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance  |
|  | 9. <input type="checkbox"/> Other _____   |

**DETAILED ACTION**

1. The communication is in response to Applicant's remarks in the amendment after final and associated amendments to the claims submitted 07/30/07. Claims 1 – 6 and 10 – 12 have been amended and are still pending. Claims 7 – 9 have been cancelled.

***Allowable Subject Matter***

2. The following is an examiner's statement of reasons for allowance: The prior art of record alone or in combination does not expressly disclose or suggest the specificity of performing cryptographic methods using discrete exponentiation in a semigroup. As for claim 1, as amended and similar claim 17, the prior art does not disclose:

...performing a first cryptographic encryption method using with the steps of:

using the verifying unit to generate a number  $t \in T$ , where  $T$  is a subrange of integers;

using the verifying unit to calculate an element  $h^{f(t)} \in H$ , where  $f: T \rightarrow T'$  is a mapping into a subrange  $T'$  of the integers, which is not necessarily different from  $T$ ,  $H$  represents a multiplicatively written semigroup generated by element  $h$ , with a discrete exponentiation of a base  $h$  as a one-way function in the semigroup  $H$ ;

using the verifying unit to calculate from the public key,  $k_{pub} = h^{f(d)} \in H$ , element  $\pi(k_{pub}^{f(t)}) \in G$ , where  $\pi: H \rightarrow G$  specifies a mapping of the semigroup  $H$  into a group  $G$ ,  $d \equiv k_{priv} \in T$  is the private key which is accessible only to the proving unit, and a mapping  $t \rightarrow h^{f(t)} \rightarrow \pi(k^{f(t)})$  from the subrange of the integers  $T$  to the group  $G$  represents a one-way function; and

using the verifying unit to encrypt the at least one data element,  $z$ , by a combination with respect to the encrypted data element,  $z' = z \circ \pi(k_{pub}^{f(t)}) \in G...$

Therefore, claims 1 – 6 and 10 – 21 are allowed.

Art Unit: 2132

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

**Conclusion**

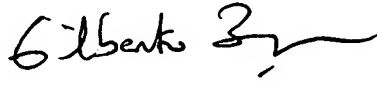
3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley  
Examiner  
Art Unit 2132

  
LLL  
01 Aug 07

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100